

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 8月20日

出 願 番 号

Application Number:

平成11年特許願第233813号

出 願 人

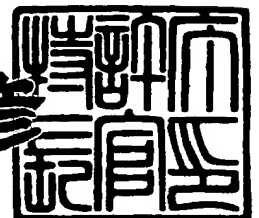
Applicant(s):

松下電器産業株式会社

2000年 6月 9日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3044854

【書類名】 特許願

【整理番号】 2022510373

【提出日】 平成11年 8月20日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 9/00

【発明者】

    【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

    【氏名】 河田 浩嗣

【発明者】

    【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

    【氏名】 勝田 昇

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

【代理人】

    【識別番号】 100097445

    【弁理士】

    【氏名又は名称】 岩橋 文雄

【選任した代理人】

    【識別番号】 100103355

    【弁理士】

    【氏名又は名称】 坂口 智康

【選任した代理人】

    【識別番号】 100109667

    【弁理士】

    【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ再生装置

【特許請求の範囲】

【請求項 1】 暗号化コンテンツを含むデジタルメディアを再生するデジタルコンテンツ再生装置で、取得した鍵を保持する鍵保持部と前記デジタルメディアの再生状況を監視する再生状況取得手段とを含み、前記暗号化コンテンツを復号するために必要な鍵データを外部より取得した後、前記鍵保持部に保存し、保存した鍵データを用いてデジタルメディアより取得した暗号化コンテンツを復号化して再生し、再生状況取得手段によって取得した前記デジタルメディアの再生状況取得手段に応じて前記鍵保持部に保存しておいた鍵データを破棄するようなデジタルコンテンツ再生装置。

【請求項 2】 鍵データで暗号化された暗号化コンテンツを含むデジタルメディアを再生するデジタルコンテンツ再生装置で、取得した鍵を保持する鍵保持部と前記デジタルメディアの再生状況を監視する再生状況取得手段と、前記鍵データを用いて前記暗号化コンテンツを復号化するコンテンツ復号化手段を含み、前記デジタルコンテンツ再生装置の外部より前記鍵データを取得した後、前記鍵保持部に保存し、前記デジタルメディアより取得した前記暗号化コンテンツを前記鍵保持部に保存した前記鍵データを用いて、前記コンテンツ復号化手段で復号化し再生し、前記再生状況取得手段を用いて取得した前記デジタルメディアの再生状況に応じて前記鍵保持部に保存していた前記鍵データを破棄するようなデジタルコンテンツ再生装置。

【請求項 3】 デジタルメディアは DVD である請求項 2 記載のデジタルコンテンツ再生装置。

【請求項 4】 デジタルコンテンツ再生状況取得手段により、デジタルコンテンツの再生状況が STOP STATE になった時点で鍵保持手段に保持していた鍵データを破棄するような請求項 3 記載のデジタルコンテンツ再生装置。

【請求項 5】 コンテンツ鍵で暗号化された暗号化コンテンツと、前記コンテンツ鍵をコンテンツ鍵復号鍵で暗号化した暗号化コンテンツ鍵とを含むデジタルメディアを再生するデジタルコンテンツ再生装置で、鍵保持手段と、デジタルコン

コンテンツ再生状況取得手段と、暗号化コンテンツ鍵復号化手段と、暗号化コンテンツ復号化手段とを具備し、前記デジタルコンテンツ再生装置の外部から前記コンテンツ鍵復号鍵を取得し、取得した前記コンテンツ鍵復号鍵を前記鍵保持手段で保持し、前記デジタルメディアから取得した前記暗号化コンテンツ鍵を、前記鍵保持手段で保持していた前記コンテンツ鍵復号鍵と前記暗号化コンテンツ鍵復号化手段とを用いて復号化してコンテンツ鍵を取得し、取得したコンテンツ鍵と前記暗号化コンテンツ復号化手段とを用いて、前記デジタルメディアから取得した暗号化コンテンツを復号化して平文コンテンツを取得し再生し、前記デジタルコンテンツ再生状況取得手段により、デジタルコンテンツの再生状況に応じて前記鍵保持手段に保持していた前記コンテンツ鍵復号鍵を破棄するようなデジタルコンテンツ再生装置。

【請求項 6】 デジタルメディアは DVD である請求項 5 記載のデジタルコンテンツ再生装置。

【請求項 7】 デジタルコンテンツ再生状況取得手段により、デジタルコンテンツの再生状況が STOP STATE になった時点で鍵保持手段に保持していたコンテンツ鍵復号鍵を破棄するような請求項 6 記載のデジタルコンテンツ再生装置。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明はデジタルメディア上に存在する暗号化されているデジタルコンテンツを取得し復号化して再生する機能を有するデジタルコンテンツ再生装置に関する。

##### 【0002】

#### 【従来の技術】

従来のこの分野のデジタルコンテンツ再生装置を、図 2 を用いて説明する。図 2 は 1 0 0 0 で示す鍵保持部と 1 1 0 0 で示すデジタルコンテンツ再生装置と 1 2 0 0 で示すデジタルメディアからなるシステムを示す。鍵保持部（1 0 0 0）には 1 0 0 1 で示す制御部と、デジタルメディアに存在する暗号化コンテンツ（

1202)を復号化するコンテンツ鍵(1002)が備わっている。デジタルコンテンツ再生装置(1100)には1101で示す制御部と1102で示すコンテンツ鍵保持部と、1104で示す読み出し手段と、1105で示す暗号化コンテンツ復号化手段と、1106で示す再生部と、1107で示す新業種津力部と、1108で示すユーザ操作入力手段が備わっている。デジタルメディア(1200)には1202で示す暗号化コンテンツが備わっている。デジタルメディアにある暗号化コンテンツ(1202)はコンテンツ鍵(1002)で暗号化されている。

#### 【0003】

以上のシステムでデジタルコンテンツ再生装置(1100)の動作を説明する。デジタルコンテンツ再生装置(1100)が、ユーザ操作入力手段(1108)によってユーザからデジタルメディア(1200)のコンテンツの再生を指示された場合を考える。デジタルコンテンツ再生装置(1100)は暗号化コンテンツ(1202)の再生に際してデジタルコンテンツ再生装置(1100)の制御部(1101)を用いて鍵保持部(1000)の制御部(1001)と通信して自らデジタルメディア(1200)内にある暗号化コンテンツ(1202)を再生する資格を有することを立証する。鍵保持部の制御部(1001)によって再生の資格を有する事を認証されたら、デジタルコンテンツ再生装置(1100)は鍵保持部(1000)よりコンテンツ鍵(1002)を取得しコンテンツ鍵保持部(1102)に保存する。その後デジタルコンテンツ再生装置(1100)はデジタルメディア(1200)より暗号化コンテンツ(1202)を読み出し手段(1104)によって取得し、先ほど保存しておいたコンテンツ鍵を用いて暗号化コンテンツ復号化手段(1105)で復号化し、平文コンテンツを得る。その後デジタルコンテンツ再生装置は再生部(1106)を用いて平文コンテンツを再生処理し、信号出力部(1107)から信号を出力する。以上でユーザからのコンテンツ再生指示の実行は終了する。その後、デジタルコンテンツ再生装置はユーザからの指示に応じて読み出し装置(1104)や再生部(1105)を用いてデジタルメディア上の暗号化コンテンツ(1202)を再生する。

#### 【0004】

上記のような構成をとることで、あるデジタルメディア上に存在する特定の暗号化コンテンツの再生にあたっては、鍵保持部によってデジタルコンテンツ再生装置がその暗号化コンテンツを再生する資格を有するかどうかの確認がとられる事が必要となる。この事により、資格を持たない不正なプレーヤがデジタルメディア上の暗号化コンテンツを再生することを防ぐ効果が期待できる。

【0005】

【発明が解決しようとする課題】

しかしながら従来の構成のデジタルコンテンツ再生装置においては、一度鍵保持部より特定のコンテンツの再生の資格があることが認められてコンテンツ鍵を入手して、コンテンツ鍵保存部に保存してしまえば、本来資格が無いはずの暗号化コンテンツの再生に関して、保存済みのコンテンツ鍵を用いることで不正に再生ができてしまう問題がある。

【0006】

本発明は従来の問題に鑑み、デジタルコンテンツ再生装置にデジタルメディア上の暗号化コンテンツの再生に際しては必ず外部にある暗号化コンテンツを再生するために必要な復号化鍵を含む鍵保持部より、再生の資格の有無をチェックされて、資格があると認められたデジタルコンテンツ再生装置のみが暗号化コンテンツを再生できるような仕組みを提供する事を目的とする。

【0007】

【課題を解決するための手段】

上記目的を解決するために本発明は、暗号化コンテンツを含むデジタルメディアを再生するデジタルコンテンツ再生装置で、取得した鍵を保持する鍵保持部と前記デジタルメディアの再生状況を監視する再生状況取得手段とを含み、前記暗号化コンテンツを復号するために必要な鍵データを外部より取得した後、前記鍵保持部に保存し、保存した鍵データを用いてデジタルメディアより取得した暗号化コンテンツを復号化して再生し、再生状況取得手段によって取得した前記デジタルメディアの再生状況取得手段に応じて前記鍵保持部に保存しておいた鍵データを破棄するようなデジタルコンテンツ再生装置を提案する。

【0008】

## 【発明の実施の形態】

本発明の実施の形態を図1を用いて説明する。

## 【0009】

図1は1000で示す鍵保持部と1100で示すDVDプレーヤと1200で示すDVDからなるシステムを示す。鍵保持部(1000)には1001で示す制御部と1002で示すコンテンツ鍵復号鍵が備わっている。コンテンツ鍵復号鍵はDVD上にある暗号化コンテンツ復号鍵(1201)を復号化してコンテンツ復号鍵を取り出すときに必要となる鍵である。DVDプレーヤ(1100)には1101で示す制御部と、1102で示すコンテンツ鍵復号鍵保持部と、1103で示す暗号化コンテンツ鍵復号化手段と、1104で示す読み出し手段と、1105で示す暗号かコンテンツ復号化手段と、1106で示す再生部と、1107で示す信号出力部と、1108で示すユーザ操作入力手段を備える。DVDディスク(1200)には1201で示す暗号化コンテンツ鍵と1202で示す暗号化コンテンツが備わっている。DVDディスクにある暗号化コンテンツ(1202)は平文コンテンツをコンテンツ鍵で暗号化したものであり、暗号化コンテンツ鍵(1201)はコンテンツ鍵をコンテンツ鍵復号鍵で暗号化したものである。

## 【0010】

DVDプレーヤ(1100)の再生動作を図1を用いて説明する。ユーザ操作入力手段(1108)よりDVDディスクにあるコンテンツの再生を指示された時を考える。まずDVDプレーヤは暗号化コンテンツの再生に際してDVDプレーヤの制御部(1101)を用い、鍵保持部の制御部(1001)と通信して自らがDVDディスク(1200)内にあるコンテンツを再生する資格を有することを立証する。鍵保持部の制御部(1001)によって再生の資格を有することを認証されたら、DVDプレーヤ(1100)は鍵保持部(1000)よりコンテンツ鍵復号鍵を取得し、コンテンツ鍵復号鍵保持部(1102)に保存する。その後DVDプレーヤ(1100)はDVDディスク(1200)より読み出し手段(1104)を用いて暗号化コンテンツ鍵を取得し、コンテンツ鍵復号鍵保持部(1102)に保存していたコンテンツ鍵復号鍵を用い暗号化コンテンツ鍵



復号化手段(1103)で、取得した暗号化コンテンツ鍵を復号化しコンテンツ鍵を取得する。その後DVDプレーヤ(1100)は読み出し手段(1104)を用いて暗号化コンテンツを取得し、先ほど取得したコンテンツ鍵を用い暗号化コンテンツ復号化手段(1105)で、取得した暗号化コンテンツを復号化し、平文コンテンツを取得する。次にDVDプレーヤ(1100)は取得した平文コンテンツを再生部(1106)を用いて再生し、信号出力部(1107)を用いて信号を出力する。以上でユーザからのコンテンツ再生の指示の実行は終了する。その後ユーザの指示に従い制御部は再生部(1104)や読み出し部(1106)を制御してDVDディスクのコンテンツを再生する。再生部(1106)はDVDディスクの再生状態が変化しているかどうかを常に調べ、再生状態が変化した場合は現在の再生状態を制御部(1101)に通知する。制御部(1101)は再生状態がSTOP STATEになった場合はコンテンツ鍵復号鍵保持部(1102)に指示を出して、保持していたコンテンツ鍵復号鍵を破棄する。

#### 【0011】

以上の動作を図3のフローチャートを用いて説明する。ユーザがDVDプレーヤにDVDディスクの再生を指示した場合を考える。DVDプレーヤは外部にある鍵保持部からDVDディスクの再生の資格があることについて認証を受ける。その後鍵保持部よりコンテンツ鍵復号鍵を取得し、DVDディスクにある暗号化コンテンツ鍵を復号化してコンテンツ鍵を取得する。その後DVDプレーヤは取得したコンテンツ鍵を用いてDVDディスクにある暗号化コンテンツを復号化して平文コンテンツを取得し再生する。その後DVDプレーヤは常に再生状態をチェックし、再生状態がSTOP STATEになった場合は鍵保持部より取得したコンテンツ鍵復号鍵を破棄し、動作を終了する。再生状態がSTOP STATEになっていない場合はユーザの指示があったかどうかを判断し、指示がある場合はその指示に従って動作する。そして以降は再生状態をチェックする動作から同様に繰り返す。

#### 【0012】

以上のように動作することによってDVDプレーヤは、DVDディスクにあるコンテンツの再生を開始するたびに外部の鍵保存部より暗号化コンテンツから再

生資格の認証を受けることが必要となる。

【0013】

なお、本実施の形態においては暗号化コンテンツを含むデジタルメディアの例としてDVDを利用する構成を示したが、他のデジタルメディアを利用する構成であっても良い。

【0014】

なお、本実施の形態においては暗号化コンテンツの復号化に際し、コンテンツ鍵復号化鍵(1002)と、コンテンツ鍵の2つの鍵を必要とする構成を示したが、特に2つの鍵で暗号化する必要は無く、2つ以上の鍵で暗号化し、その内の一つ以上を外部の鍵保持部(1000)に持たせるような構成をとっても良いし、1つの鍵で暗号化しその鍵を外部の鍵保持部(1000)に持たせるような構成をとっても良い。

【0015】

なお、本実施の形態においては、STOP STATEという状態になった場合に外部から取得した復号化鍵を破棄するような構成をとっているが、デジタルメディアの再生状況の他のいずれの場合においても、その状況に応じて外部から取得した復号化鍵を破棄するような構成をとっても良い。

【0016】

【発明の効果】

以上のように本発明の、暗号化コンテンツを含むデジタルメディアを再生するデジタルコンテンツ再生装置で、取得した鍵を保持する鍵保持部と前記デジタルメディアの再生状況を監視する再生状況取得手段とを含み、前記暗号化コンテンツを復号するために必要な鍵データを外部より取得した後、前記鍵保持部に保存し、保存した鍵データを用いてデジタルメディアより取得した暗号化コンテンツを復号化して再生し、再生状況取得手段によって取得した前記デジタルメディアの再生状況取得手段に応じて前記鍵保持部に保存しておいた鍵データを破棄するようなデジタルコンテンツ再生装置を用いることで、デジタルコンテンツ再生装置に暗号化コンテンツの再生に際しては、必ず外部にある暗号化コンテンツを再生するために必要な復号化鍵を含む鍵保持部より再生の資格の有無を認証されて

、資格があると認められた場合にのみ認められたデジタルコンテンツ再生装置で暗号化コンテンツを再生できるような仕組みを提供することができる。

【図面の簡単な説明】

【図 1】

本発明のデジタルコンテンツ再生装置の一実施の形態を示す構成図

【図 2】

本発明における分野の従来技術の一実施の形態を示す構成図

【図 3】

本発明のデジタルコンテンツ再生装置の一実施の形態の動作を示すフローチャート

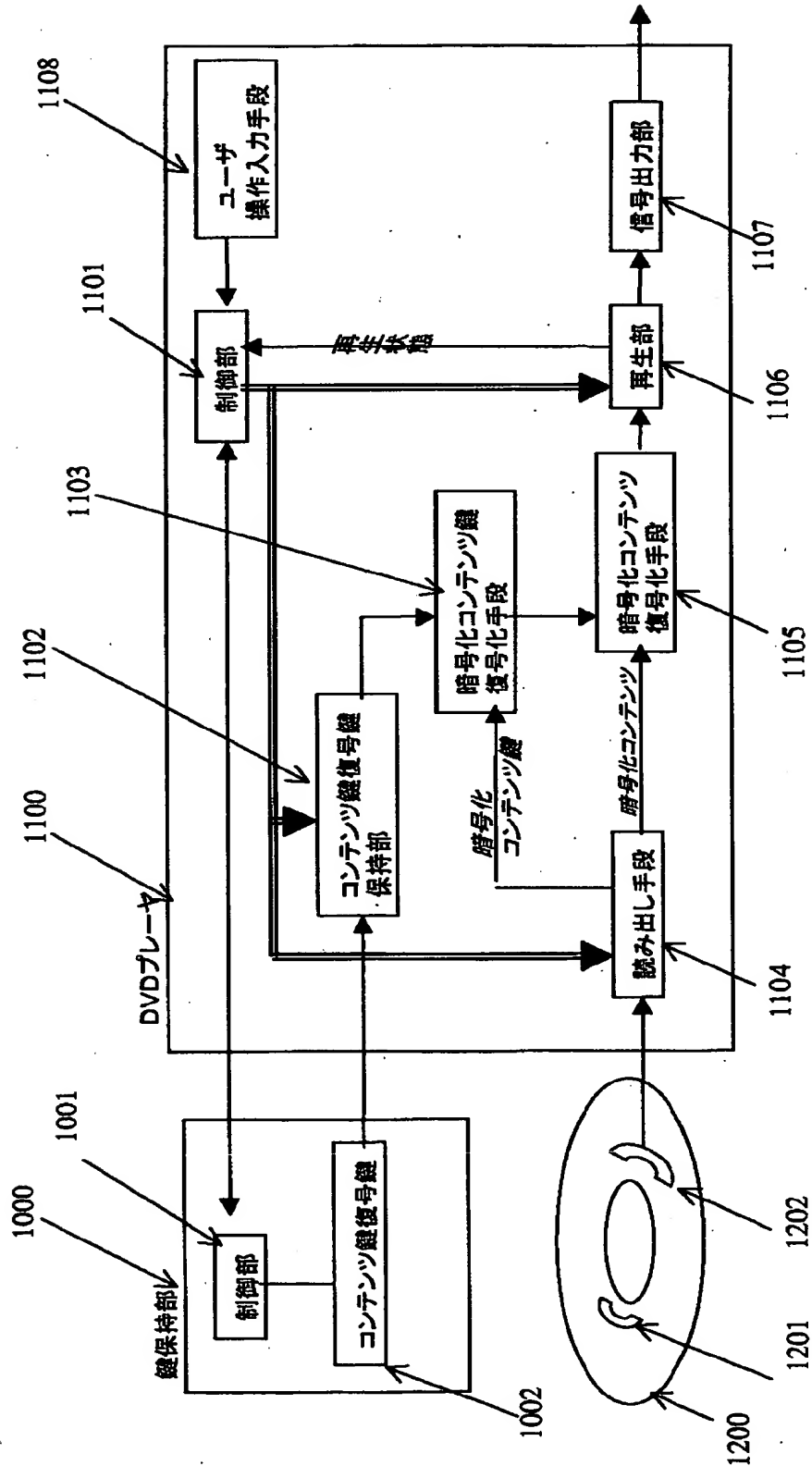
【符号の説明】

- 1000 鍵保持部
- 1001 鍵保持部の制御部
- 1002 コンテンツ鍵復号鍵
- 1100 DVDプレーヤ
- 1101 DVDプレーヤの制御部
- 1102 コンテンツ鍵復号鍵保持部
- 1103 暗号化コンテンツ鍵復号化手段
- 1104 読み出し手段
- 1105 暗号化コンテンツ復号化手段
- 1106 再生部
- 1107 信号出力部
- 1108 ユーザ操作入力手段
- 1200 DVD
- 1201 暗号化コンテンツ復号鍵
- 1202 暗号化コンテンツ

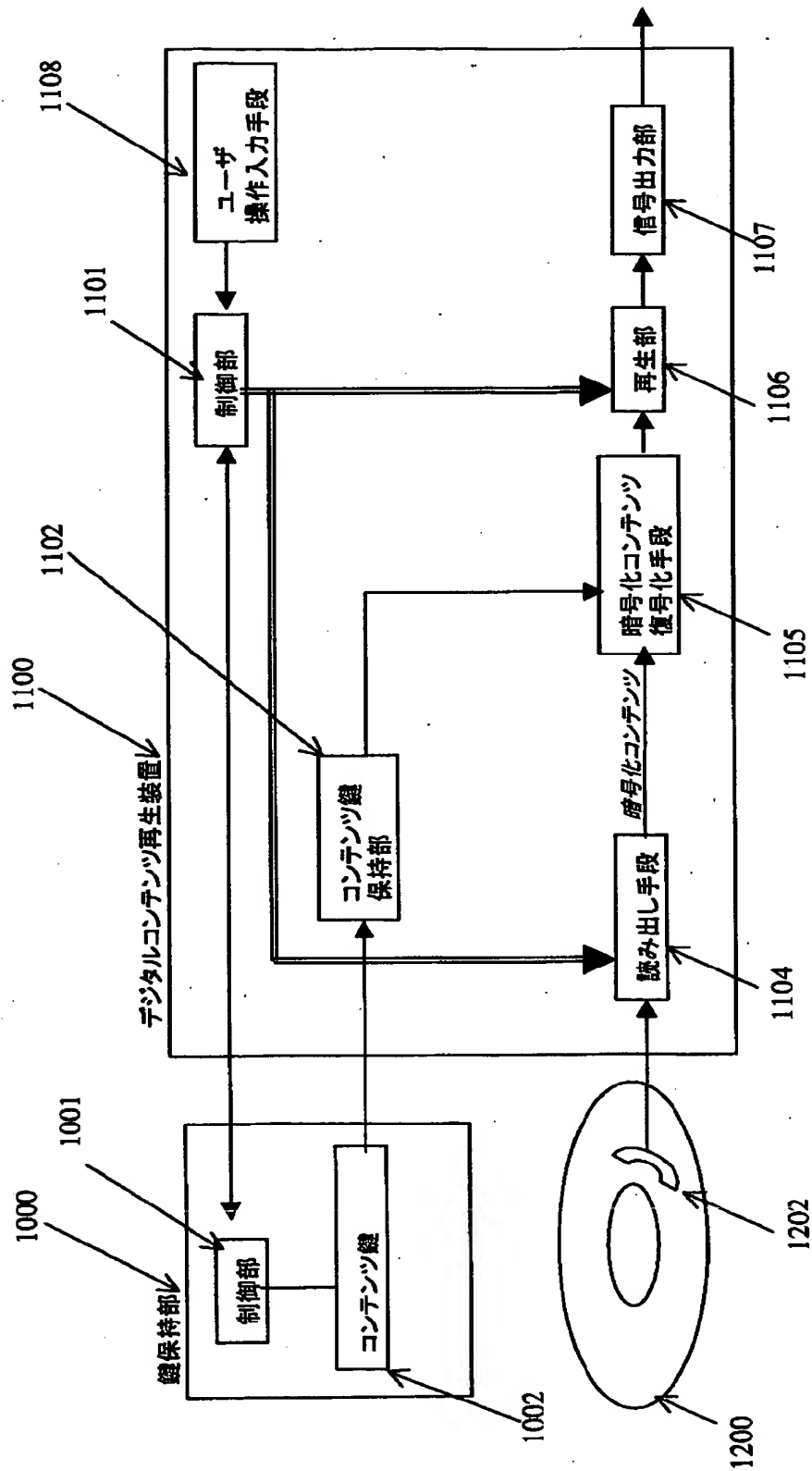
【書類名】

図面

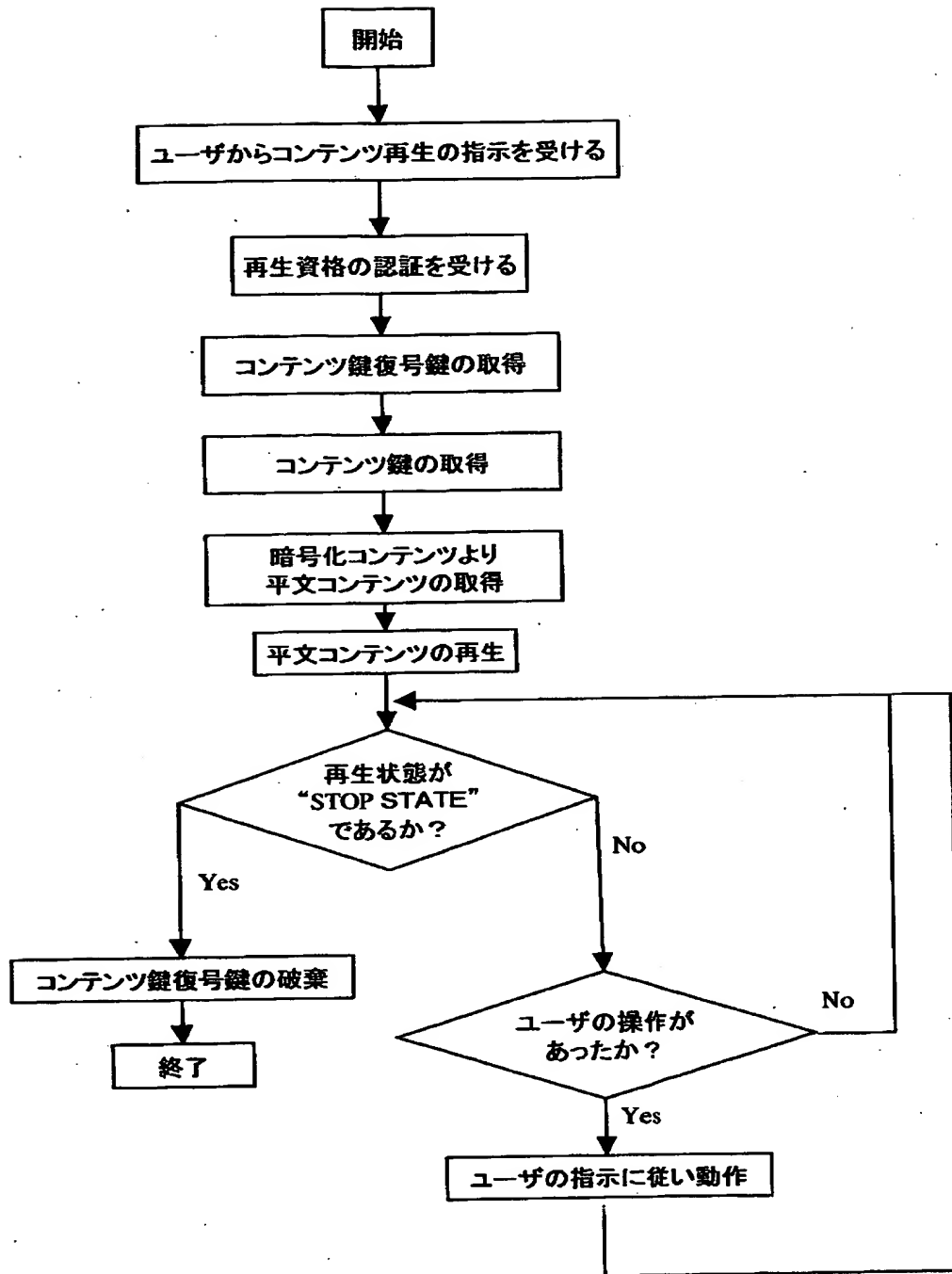
【図 1】



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】 暗号化コンテンツを含むデジタルメディアを再生するデジタルコンテンツ再生装置の内、暗号化コンテンツの再生のために装置外部より暗号化コンテンツを再生するために必要な復号鍵を取得し、復号化して再生するような装置の従来の構成においては、入手済みのコンテンツ復号鍵を用いることによって、本来資格が無いはずのコンテンツまで再生できるという課題があった。

【解決手段】 デジタルコンテンツ再生装置（1 1 0 0）の制御部は、デジタルメディア（1 2 0 0）の再生状況を監視し、デジタルコンテンツの再生状況が例えばSTOP STATE等の特定の状態に陥った場合に、コンテンツ鍵復号鍵保持部（1 1 0 2）に保持していた鍵を破棄する。以上の構成を取ることで、暗号化コンテンツの再生に関して、その都度必ず鍵保持部（1 0 0 0）より鍵を取得する事が必要となる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社